



Department of Homeland Security Daily Open Source Infrastructure Report for 06 December 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- Aero–News Network reports a 2002 Cessna T182, registration N184TA, was stolen from its hangar last month at California's El Monte Airport, the second time in two years a plane has been taken from the airport, located east of the Los Angeles basin. (See item [5](#))
- The Associated Press reports the water in a new well near the spent–fuel pool at the Indian Point 2 nuclear power plant in Buchanan, New York, is contaminated with radioactive tritium at a level 30 times higher than the federal standard for drinking water. (See item [19](#))
- The Associated Press reports Connecticut homeland security officials were left out of the communications loop for more than two hours on Friday, December 2, after a series of bomb threats forced the evacuation and shutdown of the state's 45 courthouses. (See item [24](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://www.esisac.com>]

1. *December 05, Associated Press* — **Oil pipeline blown up in Venezuela.** An explosion that damaged an oil pipeline supplying Venezuela's largest refinery was caused by government foes attempting to disrupt congressional elections, officials said. The state oil company, Petroleos de Venezuela S.A., said Monday, December 5, that the blast on Saturday, December 3, had not

forced any reduction in output because the refinery has enough crude on hand to continue operations while the pipeline is being fixed and the oil field has capacity to store pumped crude. The pipeline provided more than a third of the oil to the giant Paraguana refining complex, one of the world's largest. But inventories of 2.8 million barrels of oil at the facility assured neither supplies to the domestic market nor exports would be affected, Oil Minister Rafael Ramirez said. Ramirez said the blast disrupted the 400,000 barrels of crude a day which the pipeline supplies to the Amuay refinery, part of the giant Paraguana refining complex. Investigators found remnants of C-4 explosives at three spots on the pipeline, Interior Minister Jesse Chacon Chacon said. Venezuela is the world's fifth largest oil exporter and a major supplier to the U.S. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/05/AR2005120500788.html>

2. *December 05, KSFY TV (SD)* — **Governor asks for disaster declaration.** South Dakota Governor Mike Rounds wrote a letter Sunday, December 4, asking for federal help for recovery efforts after last week's storms affected the area. The money would help reimburse state, tribal and local units of government as well as rural electric cooperatives. The storm left 25 counties with crippled power systems. Meantime, as of Sunday afternoon state leaders say about 11,700 customers still did not have electricity. Crews have restored power to more than 79 percent of customers across the state. Officials say of the 157 communities that lost power, 16 still don't have electricity. Power has been restored to many communities, but many only have temporary generators or line hook-ups. The Governor says he expects several more small outages in the coming months because it will take some time to get permanent power restored. Damage is limited to the electric distribution system. The electric transmission system is operational. Source: <http://www.ksfy.com/Stories/Story.cfm?SID=5257>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

3. *December 05, vnunet.com* — **Fraud hits UK tax credit Website.** HM Revenue and Customs (HMRC) has announced that it has shut down its online application Website as a result of a \$52 million fraud. The department said that it has identified and prevented attempts to defraud the Tax Credits system by making claims through the tax credits e-portal. As a result it has closed the site while it develops new checks to ensure greater security. A criminal investigation has been launched into the possible misuse of a number of UK Department for Work and Pensions (DWP) staff identities in fraudulent tax credit claims. The fraud relates to internal information

held about staff and not the external records held by the DWP.

Source: <http://www.vnunet.com/vnunet/news/2147114/uk-tax-credit-webs-ite-shut-due>

4. *December 04, New York Times* — **New form of hacking raises alarms.** A hybrid form of phishing, dubbed "spear phishing," has emerged and raised alarms among the digital world's watchdogs. Spear phishing is a distilled and potentially more potent version of phishing. That's because those behind the schemes bait their hooks for specific victims instead of casting a broad, ill-defined net across cyberspace hoping to catch throngs of unknown victims. Spear phishing, say security specialists, is much harder to detect than phishing. Fake e-mail messages and Websites not only look like near perfect replicas of communiqués from e-commerce companies like eBay or its PayPal service, banks or even a victim's employer, but are also targeted at people known to have an established relationship with the sender being mimicked. Also, spear phishing is usually not the plaything of random hackers; it is more likely, analysts say, to be linked to sophisticated groups out for financial gain, trade secrets or military information. While hard data about spear phishing incidents is hard to come by and some security vendors may have a vested interest in hyping potential threats, veteran security analysts describe spear phishing as one of the more insidious cybercrimes they have encountered and one that has been under publicized because victims are hesitant to come forward.

Source: <http://www.nytimes.com/2005/12/04/business/yourmoney/04spear.html>

[[Return to top](#)]

Transportation and Border Security Sector

5. *December 05, Aero-News Network* — **Skylane stolen from El Monte airport.** A 2002 Cessna T182, registration N184TA, was stolen from its hangar last month at California's El Monte Airport. According to media reports, the theft was discovered when the plane's owner, Vincent McLeod III, went to the airport to get in some pre-Thanksgiving air time. He found the hangar empty — even the maintenance records were gone — but the two locks on the hangar door didn't appear to be broken. This is the second time in two years a plane has been taken from the airport, located east of the Los Angeles basin, according to a police detective — an alarming statistic for pilots, although plane theft was referred to as a "rarity" by the detective. The theft was reported to the Los Angeles County Terrorism Early Warning Group, according to El Monte police. Airport manager Rafael Herrera said county police told him they would begin extra patrols of the airport.

Source: <http://www.aero-news.net/index.cfm?ContentBlockID=8e969d37-36c7-4818-86e0-577ec1313509>

6. *December 05, Associated Press* — **US Airways faces challenges of combining labor forces.** After the corporate merger of American West Airlines and US Airways, one of the biggest challenges for the new US Airways — which became the nation's fifth largest domestic carrier in late September — is combining the two carriers' work forces. America West pilots have started a campaign to draw attention to their fight for seniority fairness and widely are expected to request an arbitrator to settle the issue of who ranks where in the pilot pecking order. Mechanics and ramp agents, fearing pay or benefit cuts to match the lower levels their US Airways counterparts got after the company went through bankruptcies, are fighting to retain their union and contract. Multiple negotiations are under way at once, and a smooth

combination of the two labor forces is critical to the success of the deal to combine the airlines. Union tensions and general unease about the merger are causing friction among the combined airline's 35,000 workers. Jeff McClelland, the chief administration officer of the combined company who's responsibility for labor relations, acknowledged the labor strife, but said the problem isn't widespread. Anxiety appears heaviest on the America West side of the family, which numbers more than 10,000 in the Phoenix area.

Source: <http://www.azstarnet.com/sn/hourlyupdate/105515.php>

7. *December 05, Beacon Journal (PA)* — **U.S. cities aim to launch ferries to Canada.** No fewer than three cities hope to launch U.S.-to-Canada ferry operations within a year: (1) Cleveland is eyeing a route from North Coast Harbor to Port Stanley, Ontario. (2) Grand River, near Painesville, will be the southern terminus for a Canadian company that will shuttle back and forth to Port Burwell, Ontario. (3) Erie, PA, is aiming for three ferry operations involving two Canadian ports. Whether any of these operations can sustain themselves financially is a topic of debate, given the track record of Rochester, NY. Rochester has been ferrying people and vehicles back and forth over Lake Ontario – and losing money in the process. Ray Shreckengost, executive director of the Erie Port Authority, says none of the ventures will be economically sound unless quirks in the law can be changed. For instance, he said, American ferry passengers must pay a customs tax to Canada -- something that is not required if they arrive in Canada by driving a car across a bridge (although bridge tolls are not uncommon). Ferries transporting trucks across the lake also would be hit with additional charges they would not incur if they arrived by highway, he said.

Source: <http://www.centredaily.com/mld/centredaily/news/nation/13330651.htm>

8. *December 05, New York Sun* — **Port Authority wants to divert air traffic over city to Stewart Airport.** The Port Authority of New York and New Jersey wants to divert some of the air traffic in New York City's overcrowded skies to Stewart International Airport in New Windsor, NY. The three major airports that serve New York face overcrowding in the near future, with passenger traffic expected to grow by at least 40 percent in the next 10 years. The airports are already operating at or near capacity. A quarter of the passengers who travel through the three major airports, which the Port Authority controls, face delays of an average of 50 minutes. Only John F. Kennedy International Airport, which sits on nearly 5,000 acres, has room to expand. La Guardia and Newark Liberty International airports are blocked in. Stewart International Airport, which currently serves Westchester, Dutchess, and other counties, in June announced a 20-year, \$490 million capital improvement plan to build a new passenger terminal, new taxiways, and a runway extension. Stewart International sits on more than 2,220 acres. At present it has two runways: One is 6,006 feet long and the other, at 11,818 feet, is one of the longest on the East Coast. Previously an Air Force base, Stewart International became America's first commercial airport to be privatized, in 2000.

Source: <http://www.nysun.com/article/23926>

9. *December 05, Associated Press* — **United, Denver airport reach deal on failed baggage system.** United Airlines would schedule more flights through Denver as part of a tentative deal that would erase \$184 million in its debt payments on a failed automated baggage system. The Denver City Council still must approve the deal between the Elk Grove Village, IL-based airline and Denver International Airport. The deal is likely to be attractive to the City Council because United's traffic at Denver International Airport (DIA) has been declining. "This

prevents them from diminishing the importance of the Denver hub in the United system," Stan Koniz, DIA's chief financial officer, said of the agreement. The bankrupt airline has been weighed down by \$60 million in annual payments on the baggage system, which became the butt of late night television jokes for mangling luggage. United jettisoned the system October 6 after years of using it only for luggage going from ticket counters to planes. The tentative deal announced Friday reduces the debt while securing a promise to bring more connecting passengers — and passenger fees — to the Denver airport.

Source: <http://www.usatoday.com/travel/news/2005-12-05-united-luggage-ex.htm>

[[Return to top](#)]

Postal and Shipping Sector

10. *December 05, DM News* — Rates for FedEx Ground, FedEx Home Delivery to increase.

FedEx Corp. has announced that it will increase the standard list rates for FedEx Ground and FedEx Home Delivery by an average of 3.9 percent in addition to other changes to FedEx Express, FedEx Ground, and FedEx Home Delivery surcharges effective Monday, January 2. FedEx Corp. previously announced an increase to the average shipping costs for FedEx Express by 3.5 percent. These rates are also effective January 2, and apply to U.S. domestic and U.S. export packages and freight.

Source: http://dmnews.com/cgi-bin/artprevbot.cgi?article_id=34969

11. *December 05, Manorama Online* — Cargo volume from India set to touch double-digits according to FedEx. FedEx has placed India on top of the list of fast growing markets, where it estimates that the volume of cargo is set to touch double-digit growth. Globally, the cargo volume is expected to grow 6.2 percent in the next 20 years, but in India, China, and West Asia the growth would be higher driving demand for freighter orders by cargo airlines, industry observers said in Dubai. FedEx managing director of sales and marketing for the West Asia, Indian subcontinent, and Africa said India is witnessing one of the highest global growth rates of about 25 percent.

Source: <http://www.manoramaonline.com/servlet/ContentServer?pagename=manorama/MmArticle/CommonFullStory&cid=1133612428076&c=MmArticle&p=1002194839100&count=10&colid=1002258272843&channel=News>

12. *December 05, 14 WFIE (IN)* — Indiana bomb squad diffuses suspicious package. The Evansville, IN, bomb squad was called in after a suspicious package was discovered at the downtown post office on Monday, December 5. A witness told police he saw someone go into the post office lobby, drop a backpack, and then run away. The bomb squad sent in an ANDROS robot to investigate with a camera. A water cannon was then used to diffuse the backpack, which was revealed to contain tennis shoes. The police have no idea who left the bag.

Source: <http://www.14wfie.com/Global/story.asp?S=4201433&nav=3w6o>

[[Return to top](#)]

Agriculture Sector

13. *December 05, Clarion-Ledger (MS)* — **Mississippi's oyster industry recovery could take two to three years.** When Hurricane Katrina hit the Mississippi Gulf Coast August 29, it destroyed 95 percent of the coast's adult oysters. Last year's oyster harvest brought in about \$5.5 million to local fishermen. But the storm put most of the coast's oystermen out of business. Using a \$1.5 million federal grant, the Mississippi Department of Marine Resources has employed some of the fishermen to remap the coast's oyster beds. Bradley Randall, shellfish biological program coordinator for the department, said Katrina pushed the beds around, covering some with mud and silt and raking debris across others. Using cane poles and satellite tracking devices, 67 local oystermen have spent the past month prodding the murky coastal waters. Randall said there literally are millions of baby oysters — called spat — thriving in the coastal beds. But those will take at least two years to mature, leaving a bleak outlook for next year's harvest as well.

Source: <http://www.tuscaloosanews.com/apps/pbcs.dll/article?AID=/20051205/APN/512050693&cachetime=3&template=dateline>

14. *December 04, Associated Press* — **Wasps enlisted to help ash tree.** The wasps listen for sounds of their prey, then drill through bark to reach them. Either they paralyze the juvenile victim and glue eggs to its back, or pierce it to lay the eggs inside. When the eggs hatch, the wormy wasp young munch away at leisure. The target is the larvae of the emerald ash borer (EAB), an Asian beetle that has been 100 percent fatal to North American ash trees since its arrival about 10 years ago, probably in a shipping pallet. The beetle, first noticed in 2002, has blanketed most of Lower Michigan and appeared in Ohio, Indiana, and Ontario, Canada. Worried that the bug cannot be stopped, researchers are trying to figure out how to help the ash tree survive an infestation. Scientists are studying EAB killing wasps, insecticides, cross-breeding, and the possibility of breeding a tree that makes its own insecticide. The scientists have a role model. The Asian ash tree lives alongside the beetle, but scientists there haven't studied why, so researchers here are starting from scratch. The EAB larvae feed on the cell layers beneath the bark that the tree needs to transport water and nutrients, killing it within about four years.

EAB information: <http://www.emeraldashborer.info/>

Source: <http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/1133699437311600.xml&coll=2>

15. *December 03, St. Paul Pioneer Press (MN)* — **Fifth case of bovine tuberculosis found in Minnesota beef herd.** A fifth Minnesota beef herd has tested positive for bovine tuberculosis (TB), this one in Beltrami County in northwest Minnesota, the state Board of Animal Health disclosed Friday, December 2. During preliminary tests in November, four animals in the herd showed signs of bovine TB infection, and a follow-up test confirmed the diagnosis in one animal. The outbreak is the first in Minnesota since 1971, and state officials are continuing with their program of testing, quarantines, and killing infected herds.

Source: <http://www.twincities.com/mld/twincities/business/13315910.htm>

[[Return to top](#)]

Food Sector

16. *December 05, Brownsville Herald (TX)* — **Valley leads state in food-borne illnesses.** The incidence of food-borne illnesses in the Texas Rio Grande Valley far exceeds statewide figures. State and county health officials have given a variety of answers why the Valley is a leader in food-borne illnesses. Sometimes there are just random outbreaks of diseases, which can cause a spike in reported data. Proximity to the Mexico border, where food care standards may not match those of the U.S., may also be a factor. Poverty in the Valley, which raises the question of adequate access to clean water and overcrowded living conditions may also contribute to the high number of food-related illnesses. While proximity to Mexico may be convenient to explain the high incidence of hepatitis A and salmonella in the Valley, the truth is that is an incomplete explanation. Pointing the finger south is not statistically viable, since rates for El Paso and Webb counties, which also border Mexico, do not reflect the similar numbers of cases per 100,000 people. In 2004, the rate of salmonella per 100,000 people in Texas was 11.82. In Cameron, it was 25.5 people per 100,000, while El Paso was 11.15 and Webb was 12.18. This number for Cameron over time is also higher than the other two counties, with few exceptions.

Source: http://www.brownsvilleherald.com/ts_more.php?id=68332_0_10_0_M

17. *December 03, Saginaw News (MI)* — **Luncheon illness.** Public health officials are trying to pinpoint the source of an apparent food poisoning that left four people hospitalized and 11 others ill after a church luncheon, a county official says. The Saginaw, MI, Department of Public Health remains in the midst of calling about 125 people who attended the November 20 event. As of Friday, December 2, four people remained hospitalized from dehydration and flu-like symptoms, said Bryant J. Wilke, a Health Department environmental official. Medical tests confirmed two of those people had salmonella poisoning, he said. The agency has talked to 49 others so far who reported no problems, Wilke said. Health officials learned of the problem Wednesday, November 30, when Covenant Medical Center in Saginaw notified them one of its tests to detect food poisoning turned up positive, Wilke said. The state Department of Public Health will test more.

Source: <http://www.mlive.com/news/sanews/index.ssf?/base/news-17/1133608867299390.xml&coll=9>

[[Return to top](#)]

Water Sector

18. *December 05, China Daily* — **Tap-water supply cut off as Chinese city braces for toxic slick.** On Sunday, December 4, the city of Jiamusi, in Heilongjiang, China banned the use of water for use by industries or households, fishing, swimming, or extracting ice from the Songhua River even though a toxic slick will not reach the city of 550,000 residents until noon on Tuesday, December 6. The slick has forced Harbin, a town located upstream from Jiamusi, to cut its water supply for four days. The city government is persuading the 300 households of Liushu Island to move. Wang Xianjia, the head of one of the three villages, said only about 80 people had moved to the city; and that 202 were staying put. Li Haitao, mayor of Jiamusi, has warned that pollutants are likely to be formed as a sediment along the island, resulting in long-term contamination of drinking water. The Heilongjiang Provincial Environment Protection Bureau said that 17 checking stations had been set up along the Songhua River, which were monitoring water quality around the clock.

Source: http://www.chinadaily.com.cn/english/doc/2005-12/05/content_500404.htm

19. *December 03, Associated Press* — Contamination found in new well at Indian Point.

Officials say the water in a new well near the spent-fuel pool at the Indian Point 2 nuclear power plant in Buchanan, NY, is contaminated with radioactive tritium at a level 30 times higher than the federal standard for drinking water. The well was drilled by Entergy Nuclear Northeast to find the source of a small leak from a 40-foot-deep pool which holds the highly radioactive fuel assemblies that have been used in the nuclear reactor. Critics have expressed fears that tritium could eventually work its way into drinking water supplies or into the nearby Hudson River. Entergy plans to dig eight more wells to try to map the underground flow of contaminated water as well as to find the leak.

Source: http://wcbstv.com/topstories/local_story_337200831.html

[[Return to top](#)]

Public Health Sector

20. *December 05, Agence France-Presse* — Romania quarantines suspected bird flu villages.

Two villages in the Danube delta in southeastern Romania were placed under quarantine because of fears of a bird flu outbreak, Agriculture Minister Gheorghe Flutur revealed. "As a precaution we are reacting as if these new areas have been confirmed. We have ordered the isolation of the villages of Agighiol and Crisan, and the slaughter of all poultry," Flutur told a press conference on Monday, December 5. Romanian veterinary officials on Sunday, December 4, announced that four chickens in eastern Romania were diagnosed with the H5 strain of bird flu. Tests have yet to determine if they were infected with the sub-strain of H5N1 bird flu that has killed more than 60 people in Asia. After more than a dozen outbreaks in Romania, veterinary officials expect more cases of avian flu to emerge with the arrival of waves of migrating wild birds.

Source: http://news.yahoo.com/s/afp/20051205/hl_afp/healthfluromania_051205114525;_ylt=AqiWQXpca3CyD7XR5wkDQPeJOrgF;_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCU

21. *December 04, Associated Press* — Whooping cough cases triple in Idaho. Health officials say whooping cough cases have tripled in central Idaho this year, and some districts are urging people to get revaccinated for the infectious respiratory disease. So far, 72 cases of whooping cough have been reported by the Central District Health Department, which covers Ada, Boise, Elmore, and Valley counties in southwest Idaho. About 55 of the cases so far this year have been in Ada County, the district reported, with 17 cases reported in Elmore County. That compares to the district's 10-year average of about 23 cases a year. Most people are vaccinated against whooping cough during childhood, but that vaccination can wear off by the time a person reaches adolescence. The vaccine is about 80 percent effective, officials said. Before a vaccine was available, whooping cough — otherwise known as pertussis — killed 5,000 to 10,000 people in the U.S. each year. Now, a vaccine has cut annual deaths to fewer than 30. Pertussis information: <http://www.cdc.gov/doc.do/id/0900f3ec80228696/>

Source: <http://www.jacksonholestartrib.com/articles/2005/12/04/news/regional/4031550006532a3d872570cc007e1f29.txt>

22. *December 02, The Institute for Genomic Research* — New microbial genome sheds light on sporulation. A research team led by scientists at The Institute for Genomic Research have reported the determination and analysis of the complete genome sequence of arboxydotherrnus hydrogenoformans. Isolated from a hot spring on the Russian volcanic island of Kunashir, this microbe lives almost entirely on carbon monoxide. By utilizing computational analyses and comparison with the genomes of other organisms, the researchers have discovered several remarkable features. For example, the genome encodes a full suite of genes for making spores, a previously unknown talent of the microbe. Organisms that make spores have attracted great interest recently because this is a process found in the bacterium that causes anthrax. Sporulation allows anthrax to be used as a bioweapon because the spores are resistant to heat, radiation, and other treatments. By comparing this genome to those of other spore-making species, including the anthrax pathogen, researchers identified what may be the minimal biochemical machinery necessary for any microbe to sporulate. This may help researchers better understand the biology of the bacterium that causes anthrax.
Study: <http://genetics.plosjournals.org/perlserv/?request=get-document&doi=10.1371/journal.pgen.0010065.eor>
Source: http://www.tigr.org/news/pr_12_02_05.shtml

23. *November 24, McGill University Health Center* — Blood test for major parasitic diseases. The Canadian National Reference Center for Parasitology (NRCP), based at the McGill University Health Center, is developing a comprehensive blood safety test that will allow clinicians to check for all major parasitic diseases in patients' blood. The test, which is currently in final stages of development, will also improve the safety of blood transfusions, which are one of the ways that parasitic conditions are spread. "Anyone can be bitten by an insect while on holiday and unknowingly contract a parasitic disease," says Momar Ndao, Laboratory Director of the NRCP. "For example, people with Chagas disease — caused by a parasite transmitted through the bite of the South American assassin bug — can remain symptomless for two to three decades, while the parasites slowly invade the body's organs." Conditions like the South American Chagas disease can then be transmitted to others through blood transfusions. Parasitic conditions often avoid detection because tests to identify them are often complex and expensive. The NRCP is one of only two laboratories in North America capable of conducting tests for rare parasitic conditions. The demand for testing at NRCP has increased by 270 percent over the past decade.
Source: <http://www.mcgill.ca/newswire/?ItemID=17626>

[[Return to top](#)]

Government Sector

24. *December 05, Associated Press* — Communications break down during Connecticut courthouse bomb scare. Connecticut homeland security officials were left in the dark for more than two hours Friday, December 2, after a series of bomb threats forced the evacuation and shutdown of the state's 45 courthouses, authorities acknowledged Monday, December 5. Neither police nor Governor M. Jodi Rell's office — which received one of the bomb threats at 10 a.m. EST — had informed the security agency by noon, leaving top officials to learn about the first-of-its-kind evacuation from reporters. Public Safety Commissioner Leonard Boyle said the threat fell between the cracks because it was more than a routine scare but did not rise

to level of a statewide emergency. "We're going to come up with a system, either by blast fax or e-mail, that will notify all state agencies when something like this arises," Boyle said. "When we have information that's important to get out statewide, but that isn't an emergency, we need a better way." Had a bomb exploded, James Thomas, commissioner of the Department of Emergency Management and Homeland Security would have been in charge of coordinating the response. Boyle said homeland security officials were not immediately informed because the threat was not specific, investigators couldn't determine its credibility and there was no indication of terrorism.

Source: http://www.boston.com/news/nation/articles/2005/12/05/communication_breakdown_during_conn_scare/

- 25. *December 05, Department of Homeland Security* — Johns Hopkins University to lead new Homeland Security Center.** Secretary of the Department Homeland Security Michael Chertoff announced on Monday, December 5, the selection of Johns Hopkins University (JHU) to lead a consortium studying how the nation can best prepare for and respond to potential large-scale incidents and disasters. The Department of Homeland Security anticipates providing JHU and its partners with a total of \$15 million over the next three years. This fifth Homeland Security Center of Excellence, formally titled the Center for the Study of High Consequence Event Preparedness and Response, will study deterrence, prevention, preparedness, and response, including issues such as risk assessment, decision-making, infrastructure integrity, surge capacity, and sensor networks. In particular, it will study interactions of networks and the need to use models and simulations. The Centers of Excellence, overseen by the Office of University Programs within the Homeland Security Science & Technology directorate, establish a network of university-based centers that conduct multi-disciplinary research and develop innovative educational programs. Through this initiative, the Department of Homeland Security and partner universities focus the nation's most talented researchers on homeland security issues. Additional information on Homeland Security Centers of Excellence is available at <http://www.dhs.gov/centersofexcellence>
Source: <http://www.dhs.gov/dhspublic/display?content=4957>

[[Return to top](#)]

Emergency Services Sector

- 26. *December 05, Associated Press* — Missouri fire departments fail to register.** An overwhelming majority of Missouri fire departments have failed to register with the state fire marshal, causing concern about the state's ability to coordinate a response to a large-scale incident. Local fire departments are supposed to submit their contact information, a list of their equipment and a description of their personnel capabilities each year. But for 2005, just 132 departments — out of an estimated 700 to 1,000 statewide — have complied with the registration law. State Fire Marshal Randy Cole said that when local fire agencies leave the state in the dark, it makes it more difficult to coordinate regional or statewide responses. And when departments don't register, the state cannot be sure they even exist. Department of Public Safety spokesperson Terri Durdaller said local fire agencies that don't register could jeopardize their federal grant money. They also miss out on state notices of training courses, testing opportunities, legislative initiatives and other information affecting fire departments. Missouri has required annual registration since 1988. But numerous departments have failed to register

for the past several years.

Source: http://www.bransondailynews.com/articles/2005/12/03/news/new_s3.txt

27. *December 05, Times Online (United Kingdom)* — Tsunami force ready for global role.

British police want to set up the world's first rapid-response team to identify victims of terror attacks and natural disasters around the world, based on their successful operation after the tsunami in Thailand. The extraordinary scientific jigsaw pieced together by police to identify British tourists killed by the tidal wave was revealed for the first time Monday, December 5, at the opening of a mass inquest for 93 victims. So much has been learned by these investigators that British officers have held talks about setting up a task force that can be sent anywhere there are mass casualties. No overseas investigation has called on so much police manpower. So far 740 volunteers have been sent to Thailand to work in the Disaster Victim Identification center and the two mortuaries still in operation. The British teams introduced a system called Plasdata, which helped them to compare samples taken from the 3,696 bodies recovered and the tens of thousands of items of DNA evidence collected from the victims' belongings and their relatives. They found improved ways to recover DNA from deep inside the bones of victims. Specialists in dental records and fingerprinting helped to identify more than half of the bodies.

Source: <http://www.timesonline.co.uk/article/0,,2-1904863.00.html>

28. *December 04, BBC News (United Kingdom)* — Dogs wearing cameras help combat gun

crime. New recruits to the United Kingdom's Northumbria Police force are German shepherds fitted with cameras. They have been trained to help during armed sieges and wear miniature television cameras with transmitters fitted to their heads or harnesses. It means they can search buildings and relay the information back to officers. The Fido camera system also has infra-red lights, which means pictures can be provided in darkness. Pictures are seen on a receiver unit carried by the dog handler who can watch the progress of the four-legged recruits searching for armed suspects. These dogs have also been trained to leave a mobile phone at the front door of under-siege premises so officers can negotiate with suspects.

Source: <http://news.bbc.co.uk/1/hi/england/4497212.stm>

29. *December 03, Associated Press* — Missouri working to improve quake plans, official says.

When Hurricane Katrina devastated much of the Gulf Coast earlier this year, it helped shake up earthquake disaster preparedness in Missouri. Now public safety officials are retooling how the state should respond to a catastrophic disaster. Missouri Public Safety Director Mark James said Friday, December 2, that the state isn't as prepared as it should be if a quake should occur but that much is being done to get ready. "We're not where I would like us to be," James said before a meeting of a subcommittee of the state's Seismic Safety Commission in St. Louis, MO. In the past, evacuation and emergency response plans have been prepared somewhat generically to allow a response to whatever the disaster. Hurricane Katrina showed that more planning needs to be focused on the possibility of specific events, James said. James said more focus will be on evacuation, including plans if bridges are down or roads are inoperable; ways to get people water, food and shelter if it takes time to evacuate them; and faster ways for the state to respond if local emergency providers cannot.

Source: <http://www.columbiatribune.com/2005/Dec/20051203News010.asp>

[[Return to top](#)]

Information Technology and Telecommunications Sector

30. *December 05, PC Pro* — **Google fortifies Desktop Search against IE flaw.** Google has altered its Desktop Search so that it can no longer be used in digital attacks in conjunction with a flaw in Microsoft's Internet Explorer (IE). On Friday, December 2, an Israeli hacker reported having discovered a means of remotely using Google desktop search to remotely search the computers logged on to a specially built website using Microsoft's IE. Problems in the way the browser handles Cascading Style Sheets (CSS) led to a short cut round the restrictions the browser places on interaction between different domains. Hacker Matan Gillon posted proof-of-concept code last week, but now says that it now "no longer works because Google slightly changed their site's code." However, Google told reporters that the flaw is a problem with IE, rather than the search giant's software, so the CSS problem remains at large.
Source: <http://www.pcpro.co.uk/news/81024/google-fortifies-desktop-search-against-ie-flaw.html>
31. *December 05, ZDNET (United Kingdom)* — **Trojans target unpatched IE flaw.** Computer users have been warned that several Trojan horses that exploit an unpatched flaw in Internet Explorer (IE) have been discovered. Two exploits that use the recently disclosed vulnerability were reported by antivirus company Sophos on Friday, December 2. Called Clunky-B and Delf-LT, the exploits could allow malicious code to be executed remotely on a user's PC. These Trojans could "download anything, including a 'banker Trojan' that gives up your bank details," according to a Sophos spokesperson. Systems running Microsoft IE on Windows XP Service Packs 1 and 2 are vulnerable to attack. Machines running Windows 98, Windows 98 SE, Windows Me and Windows 2000 Service Pack 4 are also vulnerable to the exploits. Microsoft is not due to issue another round of security patches until Tuesday, December 13. Some security experts have suggested the company should roll out an unscheduled patch before this time to address this flaw. However, it's not clear whether the flaw will even be addressed in the next Microsoft security bulletin. Sophos advised users to turn off the Active Scripting facility in IE, as a stop-gap measure.
Source: <http://news.zdnet.co.uk/0,39020330,39240189,00.htm>
32. *December 03, FrSIRT* — **Cisco products OpenSSL insecure protocol negotiation vulnerability.** A vulnerability has been identified in various Cisco products, which could be exploited by attackers to bypass certain security restrictions. This issue is due to an error in the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option of OpenSSL that does not properly reject SSL 2.0 sessions when a client supports SSL 3.0 or TLS 1.0, which could be exploited by malicious people to conduct MITM (Man in the Middle) attacks and force a client and a server to negotiate the SSL 2.0 protocol instead of SSL 3.0 or TLS 1.0.
Source: <http://www.frsirt.com/english/advisories/2005/2710>
33. *December 02, CNET News* — **Sober worm stalls MSN, Hotmail.** A variant of Sober known as Win32/Sober.Z@mm is to blame for disrupting e-mail traffic between Comcast account holders and user's of Hotmail and MSN Friday, December 2. These Microsoft-based e-mail servers are getting pummeled with an "unusually high mail load," causing delays in e-mail delivery to Hotmail and MSN customers, said Brooke Richardson, MSN's lead product manager. Richardson also indicated that Internet service providers besides Comcast may be having problems directing e-mail to Hotmail and MSN servers. "We are working with Comcast

and other ISPs to address [the] issues," Richardson said. Blog reports say that some Comcast subscribers, when sending e-mail to a Hotmail or MSN account, have received an error message saying their message was not received. However, Microsoft says that all e-mails, while some may be delayed, are eventually getting through.

Source: http://news.com.com/Sober+worm+stalls+MSN,+Hotmail/2100-7349_3-5980987.html?part=rss&tag=5980987&subj=news

34. *December 02, Security Focus* — **Federal flaw database commits to grading system.** A federal database of software vulnerabilities funded by the U.S. Department of Homeland Security has decided on a common method of ranking flaw severity and has assigned scores to the more than 13,000 vulnerabilities currently contained in its database, the group announced last week. The National Vulnerability Database (NVD), unveiled in August, completed its conversion over to the Common Vulnerability Scoring System (CVSS), an industry initiative aimed at standardizing the severity rankings of flaws. The CVSS gives vulnerabilities a base score based on their severity, a temporal score that measures the current danger — which could be lessened by a widely available patch, for example — and an environmental score that measures an organization's reliance on the vulnerable systems. The move to the CVSS gives the flaw-ranking initiative a major boost. Created by security researchers at networking giant Cisco, vulnerability management software provider Qualys and security company Symantec, the CVSS has not been used widely, though many companies are considering scoring flaws with the system. To date, no software vendor has yet graded vulnerabilities in its product using the CVSS.

Source: <http://www.securityfocus.com/news/11360>

35. *December 02, Federal Computer Weekly* — **Federal identification cards may get faster, safer.** By the end of December, the federal government is expected to pick a new storage standard for fingerprint data on its new Personal Identity Verification cards, a Department of Homeland Security (DHS) official said Friday, December 2. The cards are expected to use a mathematical template of fingerprint images of cardholders' two index fingers, instead of compressed images of the prints themselves, said Kevin Crouch, portfolio manager for Homeland Security Presidential Directive 12 implementation at DHS' Joint Office of Interoperable Communications. The switch breaks the nearly year-long deadlock over whether the PIV cards should use images or templates, said Walter Hamilton, chairman of the International Biometric Industry Association and vice president and general manager of biometric solutions at Saflink. The decision marks a victory for the biometrics industry, which supports using templates. Templates require less data and processing time and protect the privacy of data better than images do, Hamilton said. The National Institute of Standards and Technology supported using compressed images because the template technology is less tested than image technology.

Source: <http://www.fcw.com/article91576-12-02-05-Web>

36. *December 02, Associated Press* — **Telecom companies required to save logs of e-mail, phone calls under European Union anti-terror plan.** European Union (EU) justice and interior ministers agreed Friday, December 2, on plans that would require telecommunications companies to retain records of phone calls and e-mails for a minimum of six months for use in investigations of terrorism and other serious crimes. Britain's Home Secretary Charles Clarke, who chaired the meeting, said the deal among the 25 European Union nations allowed

governments to decide how long telecom companies in their nations should retain the data, as long as it was between six and 24 months. "We have agreed to a system which gives flexibility to member states who want to go further," Clarke told a news conference. Clarke said terrorist groups, drug dealers and people-trafficking gangs would better be targeted under the new rules. Clarke said he was optimistic the European Parliament would adopt the bill later this month -- meaning it could come into force next year. The data-tracking plan was among 12 priority measures EU governments are pushing through in the wake of July attacks on London's transportation system.

Source: <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/13312628.htm>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT has received reports of a phishing email scam that attempts to convince the user that it is from the Internal Revenue Service (IRS) by using a spoofed "From" address of "tax-refunds@irs.gov".

Upon clicking on the link provided in the email, the user is taken to a fraudulent site that looks like a legitimate U.S. government site. The user is then asked to provide personal information, such as their social security, credit card and bank pin numbers.

Users are encouraged to take the following measures to protect themselves from this type of phishing attack:

Do not follow unsolicited web links received in email messages.

Contact your financial institution immediately if you believe your account/and or financial information has been compromised.

For additional information on ways to avoid phishing email attacks, US-CERT recommends that all users review the following:

Avoiding Social Engineering and Phishing Attacks at URL:

<http://www.us-cert.gov/cas/tips/ST04-014.html>

Spoofed/Forged Email at URL: http://www.cert.org/tech_tips/email_spoofing.html

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 1025 (win-rpc), 554 (rtsp), 2745 (Bagle.C), 1434 (ms-sql-m), 1433 (ms-sql-s), 4899 (radmin), 1026 (win-rpc)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

37. *December 04, Associated Press* — Arkansas man climbs White House fence. A man from Arkansas climbed the fence surrounding the White House Sunday, December 4, while President Bush was inside, and was immediately captured by Secret Service officers. Secret Service spokesperson Jonathan Cherry identified the climber as Shawn A. Cox. Cherry said Cox was being charged with unlawful entry and was expected to appear Monday in U.S. District Court. Cox has previously come to the attention of the Secret Service, Cherry said. Cherry said he did not know where Cox was from in Arkansas or why he wanted to get on the White House grounds. He did not have a weapon, Cherry said. Uniformed Secret Service officers stood by with guns drawn while an agent escorted Cox to a guard station.

Source: <http://www.cnn.com/2005/US/12/04/whitehouse.security.ap/index.html>

[[Return to top](#)]

General Sector

Nothing to report.

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.